(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 605 070 A2**

(12) # EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: 93250344.4

(51) Int. Cl.5: G07F 7/10

(22) Anmeldetag: 13.12.93

(30) Priorität: 23.12.92 DE 4243851

(43) Veröffentlichungstag der Anmeldung:
06.07.94 Patentblatt 94/27

(84) Benannte Vertragsstaaten:
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

(71) Anmelder: DEUTSCHE BUNDESPOST TELEKOM
Godesberger Allee 87-93
D-53175 Bonn(DE)
Anmelder: INTERNATIONAL BUSINESS MACHINES CORPORATION
Old Orchard Road
Armonk, N.Y. 10504(US)
Anmelder: ORGA DATENTECHNIK GmbH
Nordstrasse 26
D-33102 Paderborn(DE)
Anmelder: GAD GESELLSCHAFT FUR AUTOMATISCHE DATENVERARBEITUNG EG
Postfach 3048
D-4400 Münster(DE)

(72) Erfinder: Endler, Reinhard
Behringstrasse 31
D-90542 Eckental(DE)
Erfinder: Westphal, Reinhard
Sprangerstrasse 16
D-90574 Rosstal(DE)
Erfinder: Hartleif, Siegfried
Heinrich-Heine-Strasse 18A
D-64823 Gross-Umstadt(DE)
Erfinder: Niehaus, Herbert
Franz-Marc Weg 21
D-48165 Münster(DE)
Erfinder: Schäfer, Peter, GAD: Gesellschaft für automatische Datenverarbeitung EG,
Postfach 30 48
D-4400 Münster(DE)
Erfinder: Mergemeier, Detlev, GAD: Gesellschaft für automatische Datenverarbeitung EG,
Postfach 30 48
D-4400 Münster(DE)
Erfinder: Hovemeyer, Dieter, Orga Datenverarbeitung EG
Nordstrasse 26
D-33102 Paderborn(DE)

(74) Vertreter: Strehse, Rainer et al
Deutsche Bundespost Telekom,
Forschungs-und Technologiezentrum,
Ref. Z 33,
Postfach 1.13
D-10108 Berlin (DE)

(54) **Verfahren zum Transferieren von Buchgeldbeträgen auf und von Chipkarten.**

(57) **2.1.** Bei bekannten Verfahren wird davon ausgegangen, daß debitorische und kreditorische Börsenfunktionen unabhängig voneinander arbeiten. Der erfindungsgemäßen Lösung liegt die Aufgabe zugrunde, die Vorteile der kreditorischen Börse mit den Vorteilen der debitorischen Börse zu vereinen.

2.2. Erfindungsgemäß werden überschreibbare Speicherplätze einer Chipkarte in einen Speicherplatz für kreditorische Börsenfunktionen und mindestens einen Speicherplatz für debitorische Börsenfunktionen aufgeteilt. Über das Applikationsprogramm der Chipkarte wird in Verbindung mit dem Programm eines Autorisierungssystems ein Buchgeldbetrag aus der kreditorischen Börse, einmalig oder mehrfach hintereinander, in die debitorische Börse transferiert.

2.3. Durch die erfindungsgemäße Lösung ist der Dienstenutzer in der Lage, mittels nur einer multifunktionalen Chipkarte, jederzeit aus dem ihm im Rahmen der kreditorischen Börse gewährten Kredit die debitorische Börse der Chipkarte aufzufüllen.

EP 0 605 070 A2

schen und kreditorischen Börse angezeigt. Parallel dazu findet sowohl eine Authentifikation der Chipkarte gegenüber dem Autorisierungssystem, als auch eine Authentifikation des Autorisierungssystems gegenüber der Chipkarte durch geeignete kryptographische Verfahren statt.

Wenn der Dienstenutzer sich zum Auffüllen seiner debitorischen Börse entschließt, wird durch das Auslösen eines dementsprechenden Befehls durch den Dienstenutzer der Umbuchungsvorgang ausgelöst. Dabei werden zunächst weitere Daten der debitorischen Börse der Chipkarte über das Endgerät an das Autorisierungssystem übertragen.

Anhand des Programms des Autorisierungssystem wird überprüft, ob das Verfallsdatum der debitorischen Börse abgelaufen ist, ob die Seriennummer in einer Sperrliste steht und ob mit dem Aufladevorgang das Limit des Geldbetrages für die debitorische Börse überschritten wird. Bei erfolgreicher Prüfung über das Programm des Autorisierungssystems erfolgt ein Auslesen weiterer Daten der kreditorischen Börse der Chipkarte.

Über das Programm des Autorisierungssystems wird ebenfalls geprüft, ob das Verfallsdatum der kreditorischen Börse abgelaufen ist, ob die Seriennummer in einer Sperrliste steht und ob der Kreditrahmen bei Abbuchung der gewünschten Summe gewahrt bleibt.

Anschließend wird der Dienstenutzer durch das Programm des Autorisierungssystems über das Endgerät zur Eingabe seiner persönlichen Geheimzahl PIN aufgefordert. Durch Eingabe der PIN und bei erfolgreicher Überprüfung durch die Chipkarte erfolgt über den kryptographisch gesicherten Abbuchungsbefehl, der vom Autorisierungssystem über das Endgerät zur Chipkarte übertragen wird, die Abbuchung des gewünschten Buchgeldbetrages aus der kreditorischen Börse.

Als Quittung über die Abbuchung des Buchgeldbetrages von der kreditorischen Börse wird mittels des Applikationsprogrammes der Chipkarte über das Endgerät ein kryptographisch gesicherter Buchungsdatensatz erstellt, der vom Dienstebetreiber der debitorischen Börse zur Verrechnung beim Diensteanbieter der kreditorischen Börse eingereicht wird. Gleichzeitig wird ein Message-Authentifikations-Code MAC übertragen. Der MAC wird gebildet, indem die Klartextdaten des Buchungsdatensatzes mit einem in der Chipkarte vorhandenen Schlüssel des Dienstebetreibers der kreditorischen Börse verschlüsselt werden. Mit dem MAC überprüft der Dienstebetreiber der kreditorischen Börse die Echtheit des Buchungsdatensatzes, indem er den MAC entschlüsselt und die Daten mit den Klartexten im Buchungsdatensatz vergleicht.

Nach Prüfung des Buchungsdatensatzes wird der aus der kreditorischen Börse abgebuchte Buchgeldbetrag (zuzüglich MAC) ebenfalls kryptographisch gesichert, vom Autorisierungssystem über das Endgerät in die debitorische Börse geladen.

Die Quittung über den in die debitorische Börse der Chipkarte geladenen Buchgeldbetrag zuzüglich MAC erfolgt wiederum in Form einer MAC-gesicherten Bestätigung, genannt MAC'. Sie wird kryptographisch gesichert über das Endgerät zum Autorisierungssystem übertragen.

Mit dem MAC' überprüft der Dienstebetreiber der kreditorischen Börse, ob dem Dienstenutzer auch tatsächlich die Dienstleistung, nämlich das Laden des aus der kreditorischen Börse entnommenen Buchgeldbetrages in die debitorische Börse, erbracht wurde.

Patentansprüche

1. Verfahren zum Transferieren von Buchgeldbeträgen auf und von Chipkarten mit mindestens zwei überschreibbaren Speicherplätzen, unter Verwendung von Diensteanbieter-Endgeräten, die mit einem Autorisierungssystem verbindbar sind, wobei bekannte Verfahren, sowohl für die Buchung als auch für die kryptographisch abgesicherte Erstellung von Buchungsquittungen zum Einsatz kommen,
   dadurch gekennzeichnet, daß die überschreibbaren Speicherplätze der Chipkarte in einen kreditorischen und mindestens einen debitorischen Speicherplatz aufgeteilt werden, wobei über das Applikationsprogramm der Chipkarte in Verbindung mit dem Programm eines Autorisierungssystems ein in einem vorgegebenen Kreditrahmen beliebig oft wiederholbares Umbuchen von Buchgeldbeträgen aus dem Speicherbereich für kreditorische Börsenfunktion in den Speicherbereich für debitorische Börsenfunktion realisiert wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß nach dem Eingeben der Chipkarte in ein Endgerät eines Dienstebetreibers dem Dienstenutzer der aktuelle Stand der debitorischen und kreditorischen Börse angezeigt wird,
   - daß parallel zur Anzeige der Beträge eine Authentifikation der Chipkarte gegenüber dem Autorisierungssystem, als auch eine Authentifikation des Autorisierungssystems gegenüber der Chipkarte durch geeignete kryptographische Verfahren stattfindet,
   - daß nach Auslösen des Umbuchungsvorganges durch den Dienstenutzer zum Auffüllen der debitorischen Börse zunächst weitere Daten der debitorischen Börse der Chipkarte an das mit dem

Endgerät zum Autorisierungssystem übertragen wird.

- daß der MAC mit dem Schlüssel des Dienstebetreibers der kreditorischen Börse gebildet wird, so daß dieser eine Validierung des Umbuchungsvorganges vornehmen kann.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 605 070 A3**

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **93250344.4**

(51) Int. Cl.[6]: **G07F 7/10**

(22) Anmeldetag: **13.12.93**

(30) Priorität: **23.12.92 DE 4243851**

(43) Veröffentlichungstag der Anmeldung:
06.07.94 Patentblatt 94/27

(84) Benannte Vertragsstaaten:
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

(88) Veröffentlichungstag des später veröffentlichten Recherchenberichts: **08.02.95 Patentblatt 95/06**

(71) Anmelder: **DEUTSCHE BUNDESPOST TELEKOM**
Godesberger Allee 87-93
D-53175 Bonn (DE)
Anmelder: **INTERNATIONAL BUSINESS MACHINES CORPORATION**
Old Orchard Road
Armonk, N.Y. 10504 (US)
Anmelder: **ORGA DATENTECHNIK GmbH**
Nordstrasse 26
D-33102 Paderborn (DE)
Anmelder: **GAD GESELLSCHAFT FUR AUTOMATISCHE DATENVERARBEITUNG EG**
Postfach 3048
D-4400 Münster (DE)

(72) Erfinder: **Endler, Reinhard**
Behringstrasse 31
D-90542 Eckental (DE)

Erfinder: **Westphal, Reinhard**
Sprangerstrasse 16
D-90574 Rosstal (DE)
Erfinder: **Hartleif, Siegfried**
Heinrich-Heine-Strasse 18A
D-64823 Gross-Umstadt (DE)
Erfinder: **Niehaus, Herbert**
Franz-Marc Weg 21
D-48165 Münster (DE)
Erfinder: **Schäfer, Peter, GAD: Gesellschaft für automatische Datenverarbeitung EG,**
Postfach 30 48
D-4400 Münster (DE)
Erfinder: **Mergemeier, Detlev, GAD: Gesellschaft für automatische Datenverarbeitung EG,**
Postfach 30 48
D-4400 Münster (DE)
Erfinder: **Hovemeyer, Dieter, Orga Datenverarbeitung EG**
Nordstrasse 26
D-33102 Paderborn (DE)

(74) Vertreter: **Strehse, Rainer et al**
Deutsche Bundespost Telekom,
Forschungs-und Technologiezentrum,
Ref. Z 33,
Postfach 1.13
D-10108 Berlin (DE)

(54) Verfahren zum Transferieren von Buchgeldbeträgen auf und von Chipkarten.

(57) **2.1.** Bei bekannten Verfahren wird davon ausgegangen, daß debitorische und kreditorische Börsenfunktionen unabhängig voneinander arbeiten. Der erfindungsgemäßen Lösung liegt die Aufgabe zugrunde, die Vorteile der kreditorischen Börse mit den Vorteilen der debitorischen Börse zu vereinen.

2.2. Erfindungsgemäß werden überschreibbare Speicherplätze einer Chipkarte in einen Speicherplatz für kreditorische Börsenfunktionen und mindestens einen Speicherplatz für debitorische Börsenfunktionen aufgeteilt. Über das Applikationsprogramm der Chipkarte wird in Verbindung mit dem Programm eines Autorisierungssystems ein Buchgeldbetrag aus der kreditorischen Börse, einmalig oder mehrfach hintereinander, in die debitorische Börse transferiert.

2.3. Durch die erfindungsgemäße Lösung ist der Dienstenutzer in der Lage, mittels nur einer multi-

EP 0 605 070 A3

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 93 25 0344

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.5)
Y	US-A-4 859 837 (J.W. HALPERN) * Zusammenfassung; Ansprüche; Abbildung 1B * * Spalte 3, Zeile 58 - Spalte 4, Zeile 61 * ---	1	G07F7/10
Y	WO-A-90 15382 (DATACARD CORPORATION) * Zusammenfassung; Ansprüche; Abbildungen * * Seite 5, Zeile 34 - Seite 9, Zeile 33 * ---	1	
A	EP-A-0 157 416 (OMRON TATEISI ELECTRONICS) * Zusammenfassung; Ansprüche; Abbildungen 1-6,11,12 * * Seite 16, Zeile 7 - Zeile 14 * * Seite 30, Zeile 11 - Seite 36, Zeile 17 * ---	1-3	
A	US-A-4 839 504 (H. NAKANO) * Zusammenfassung; Ansprüche; Abbildungen 1,2,4,19-21 * ---	1-3	RECHERCHIERTE SACHGEBIETE (Int.Cl.5)
A	EP-A-0 172 670 (TECHNION RESEARCH & DEVELOPMENT) * das ganze Dokument * ---	1-3	G07F
A	US-A-4 007 355 (R. MORENO) -----		

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	13. Dezember 1994	David, J

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus andern Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)